Introduction

The ever-growing threat landscape has been causing major vulnerabilities within organizations. The difficulty for administrators to manage new threats while maintaining a high-level threat posture can be a hard task for even the most seasoned security administrator. Maintaining this balancing act between new and existing security threats is especially challenging in organizations that maintain hybrid environments. Microsoft Defender for Identity helps address the security needs of these organizations. Defender for Identity protects your on-premises Active Directory users and the users that are synced to your Azure Active Directory.

Important

Microsoft Defender for Identity replaces Microsoft Advanced Threat Analytics (ATA). For organizations that had previously implemented ATA, it's recommended that you transition to Microsoft Defender for Identity. While extended ATA support will last until January 2026, mainstream ATA support ended January 12, 2021. For information on transitioning from ATA to Microsoft Defender for Identity, see **Advanced Threat Analytics (ATA) to Microsoft Defender for Identity**.

In this module, you'll learn how Microsoft Defender for Identity monitors users, entity behavior, and activities with learning-based analytics. The Microsoft Defender for identity portal is used to monitor and respond to detected suspicious activity. The portal provides a quick view of all suspicious activity in chronological order. It allows administrators to filter out specific details of any activity and gives actions based on those activities. The Defender for Identity portal also shows alerts and notifications that highlight problems detected by the service.

After completing this module, you'll be able to:

- Describe how Microsoft Defender for Identity monitors users, entity behavior, and activities with learning-based analytics.
- Describe how Defender for Identity protects user identities and credentials stored in Active Directory.
- Describe how Defender for Identity identifies and investigates suspicious user activities and advanced attacks throughout the kill chain.
- Create your Microsoft Defender for Identity instance in the Defender for Identity portal.
- Use the built-in portal to monitor and respond to suspicious activity detected by Defender for Identity.

Explore Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution. It uses an organization's on-premises Active Directory information to identify, detect, and analyze potential threats, compromised accounts, and malicious insider actions inside the organization. Defender for Identity monitors not just user accounts, but all devices in an organization's network that perform authentication and authorization requests against Active Directory, including non-Windows and mobile devices. Besides analyzing an organization's Active Directory traffic using deep packet inspection technology, Defender for Identity also collects relevant Windows Events from the organization's domain controller and creates entity profiles based on information from Active Directory Domain Services.

The Defender for Identity service helps security administrators that find it challenging to detect advanced attacks that occur in a hybrid environment. To get a better understanding of Microsoft Defender for identity, this unit will review key components that make up the service and how administrators can use this service to increase the threat resilience of their organization.

What does Microsoft Defender for Identity do?

Microsoft Defender for Identity monitors an organization's domain controllers by capturing and parsing network traffic and using Windows events directly from the domain controllers. It then analyzes the data for attacks and threats. Using profiling, deterministic detection, machine learning, and behavioral algorithms, Defender for Identity learns about an organization's network, enables detection of anomalies, and provides warnings of suspicious activities.

With Defender for Identity, there's no need to create rules, thresholds, or baselines and then fine-tune. Defender for Identity analyzes the behaviors among users, devices, and resources, along with their relationship to one another. In doing so, it can quickly detect suspicious activity and known attacks.

- Defender for Identity will start detecting known malicious attacks and security issues immediately after deployment.
- Three weeks after deployment, Defender for Identity starts to detect suspicious behavioral activities.

Defender for Identity performs the following tasks:

- **Monitors and profiles user behavior and activities.** Defender for Identity monitors and analyzes user activities and information across an organization's network. This information includes permissions and group membership. In doing so, it creates a behavioral baseline for each user.

  Defender for Identity then identifies anomalies with adaptive built-in intelligence. This action provides organizations with insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing the organizations. Defender for Identity's proprietary sensors monitor organizational domain controllers, providing a comprehensive view for all user activities from every device.
- **Protects user identities and reduces the attack surface.** Defender for Identity provides invaluable insights on identity configurations and suggested security best-practices. Through security reports and user profile analytics, Defender for Identity helps dramatically reduce an organization's attack surface, making it harder to compromise user credentials and advance an attack.

  Defender for Identity's visual Lateral Movement Paths helps companies quickly understand exactly how an attacker can move laterally inside their organizations to compromise sensitive accounts and help prevent those risks in advance. The security reports generated by Defender for Identity help organizations identify users and devices that authenticate using clear-text passwords. They also provide other insights to improve an organization's security posture and policies.
- **Protects AD FS in hybrid environments.** Active Directory Federation Services (AD FS) plays important role in today's infrastructure when it comes to authentication in hybrid environments. Defender for Identity protects the AD FS in an organization's environment by detecting on-premises attacks on the AD FS and providing visibility into authentication events generated by the AD FS.
- **Identifies suspicious activities and advanced attacks across the cyber-attack kill-chain.** Most attacks are launched against an accessible entity, such as a low-privileged user. The attack then moves laterally until the attacker gains access to valuable assets – such as sensitive accounts, domain administrators, and highly sensitive data. Defender for Identity identifies the following advanced threats at the source throughout the entire cyber-attack kill chain:
  - **Reconnaissance.** Identify rogue users and attackers' attempts to gain information. Attackers use various methods to search for information about user names, users' group membership, IP addresses assigned to devices, resources, and more.

    - **Compromised credentials.** Identify attempts to compromise user credentials using brute force attacks, failed authentications, user group membership changes, and other methods.
    - **Lateral movements.** Detect attempts to move laterally inside the network to gain further control of sensitive users. It uses methods such as Pass the Ticket, Pass the Hash, Overpass the Hash, and more.
    - **Domain dominance.** Highlight attacker behavior if domain dominance is achieved through remote code execution on the domain controller, and methods such as DC Shadow, malicious domain controller replication, Golden Ticket activities, and more.
- **Investigates alerts and user activities.** Defender for Identity is designed to reduce general alert noise. It provides only relevant, important security alerts in a simple, real-time organizational attack timeline. The **Defender for Identity attack timeline** view enables organizations to easily stay focused on what matters by using the intelligence of smart analytics.

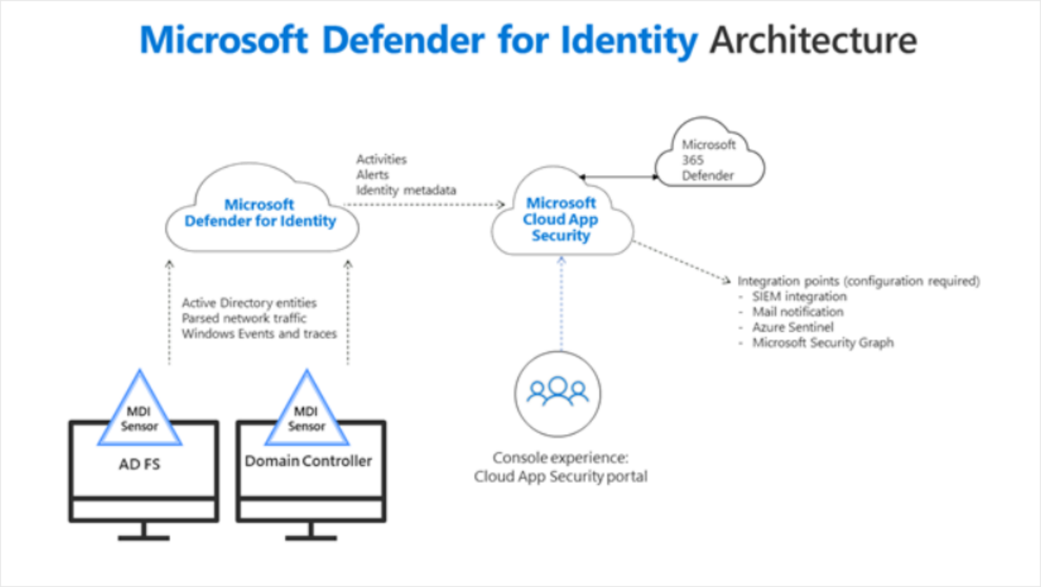
  Defender for Identity can quickly investigate threats and gain insights across the organization for users, devices, and network resources. Integration with Microsoft Defender for Endpoint provides another layer of enhanced security. It does so by providing detection and protection against advanced persistent threats on the operating system.

Defender for Identity architecture

Using profiling, deterministic detection, machine learning, and behavioral algorithms, Defender for Identity learns about an organization's network, enables detection of anomalies, and provides warnings of suspicious activities. It provides these services through the integration of the following key components:

- **Defender for Identity portal.** The Defender for Identity portal enables an organization to create its Defender for Identity instance. The portal also displays the data received from Defender for Identity sensors, and enables an organization to monitor, manage, and investigate threats in its network environment.
- **Defender for Identity sensor.** Every domain controller in a company's environment should be covered by a Defender for Identity sensor or standalone sensor. Installed directly on an organization's domain controller or AD FS servers, the Defender for Identity sensor accesses the event logs it requires directly from the servers. The sensor sends only the parsed information retrieved from the logs and network traffic to the Defender for Identity cloud service (only a percentage of the logs are sent). Defender for Identity sensors can be installed directly on the following servers:

  - **Domain controllers**. The sensor directly monitors domain controller traffic, with no dedicated server, or configuration of port mirroring.
  - **AD FS servers**. The sensor directly monitors network traffic and authentication events.
- **Defender for Identity cloud service.** Defender for Identity cloud service runs on Azure infrastructure. It's currently deployed in the US, Europe, and Asia. Defender for Identity cloud service is connected to Microsoft's intelligent security graph.


Microsoft Defender for Identity Architecture
Microsoft Defender for Identity
Activities
Alerts
Identity metadata
Microsoft Cloud App Security
Microsoft 365 Defender
Integration points (configuration required)
- SIEM integration
- Mail notification
- Azure Sentinel
- Microsoft Security Graph
Active Directory entities
Parsed network traffic
Windows Events and traces
MDI Sensor
AD FS
MDI Sensor
Domain Controller
Console experience:
Cloud App Security portal

By default, Defender for Identity supports up to 200 sensors. If you want to install more sensors, contact Defender for Identity support at Microsoft.

The Defender for Identity sensor includes a monitoring component that evaluates the available compute and memory capacity on the domain controller on which it's running. The monitoring process runs every 10 seconds and dynamically updates the CPU and memory utilization quota on the Defender for Identity sensor process. The monitoring process makes sure the domain controller always has at least 15% of free compute and memory resources available.

No matter what occurs on the domain controller, the monitoring process continually frees up resources for maintaining the domain controller's core functionality. If the monitoring process causes the Defender for Identity sensor to run out of resources, only partial traffic will be monitored and the health alert "Dropped port mirrored network traffic" appears in the Defender for Identity portal Health page.

Defender for Identity data collection

Defender for Identity collects and stores information from an organization's configured servers (domain controllers, member servers, and so on). This information is stored in a database specific to the service for administration, tracking, and reporting purposes. Information collected includes:

- network traffic to and from domain controllers (such as Kerberos authentication, NTLM authentication, and DNS queries).
- security logs (such as Windows security events).
- Active Directory information (structure, subnets, sites).
- entity information (such as names, email addresses, and phone numbers).

Microsoft uses this data to:

- Proactively identify indicators of attack in an organization.
- Generate alerts if a possible attack was detected.
- Provide an organization's security operations team with a view into entities related to threat signals from its network. This view enables the organization to investigate and explore the presence of security threats on its network.

Important

Microsoft doesn't mine your data for advertising or for any other purpose other than providing you the Defender for Identity service.

Deploying Microsoft Defender for Identity

It's recommended that organizations deploy Defender for Identity in three phases:

- **Phase 1:**
  1. Install Defender for Identity to protect your primary environments. Defender for Identity's fast deployment model enables organizations to start protecting their environments immediately.
  2. Set sensitive accounts and honey token accounts.
  3. Review reports and lateral movement paths.
- **Phase 2:**
  1. Protect all the domain controllers and forests in the organization.
  2. Monitor all alerts. Investigate lateral movement and domain dominance alerts.
  3. Work with the Security Alert guide to understand threats and triage potential attacks.
- **Phase 3:**
  1. Integrate Defender for Identity alerts into your security operation's workflows.

Create your Microsoft Defender for Identity instance

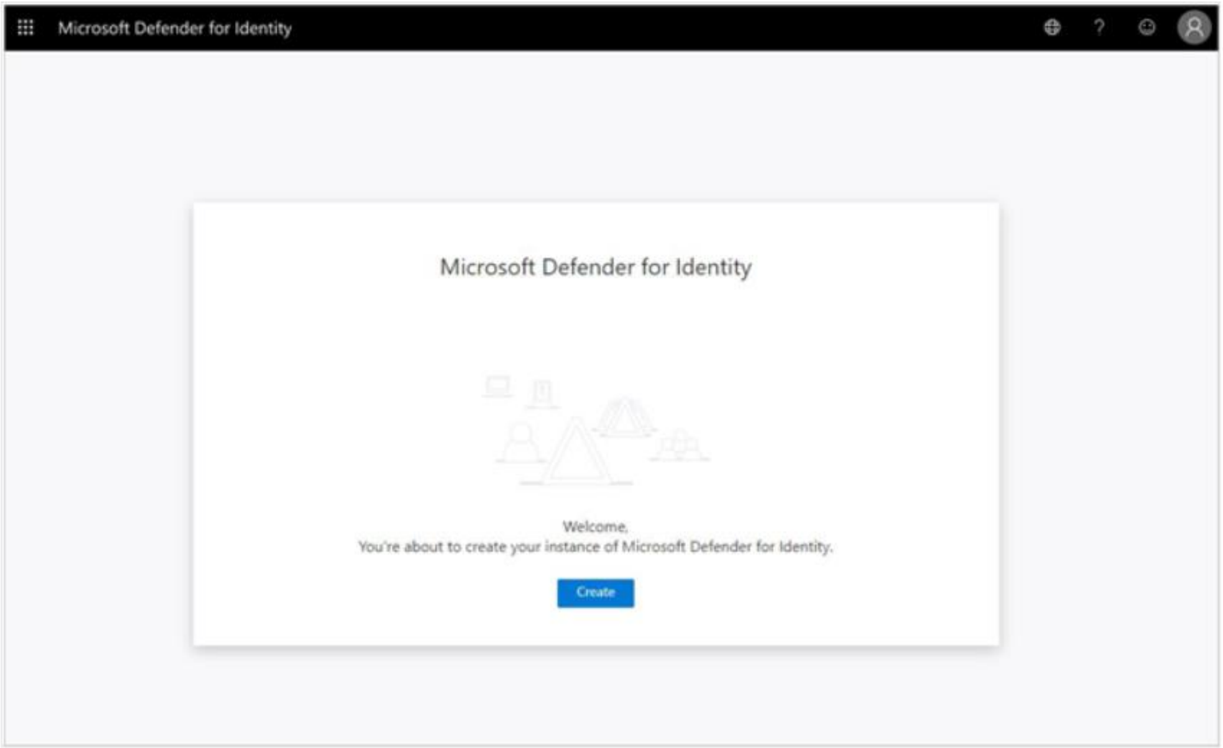
To implement Microsoft Defender for Identity, an organization must create a Defender for Identity instance (previously called a workspace). An administrator must create the instance in the Defender for identity portal. To create the Defender for Identity instance, the administrator must first satisfy the following prerequisites:

- The Administrator will need a Microsoft Defender for Identity license. This can either be an individual license or part of a licensing plan, such as an Office 365 E5 license. For more information, see Defender for Identity licensing guidance.
- The Administrator must be assigned to either a global administrator role or a security administrator role on the tenant to access the Defender for identity portal.
- The domain controller (s) you intend to install Defender for Identity sensors on must have internet connectivity to the Defender for Identity Cloud Service. The Defender for Identity sensor supports the use of a proxy. For more information on proxy configuration, see Configuring a proxy for Defender for Identity.
- One of the following directory services accounts must have read access to all objects in the monitored domains:
  - **A standard AD user account and password.** Required for sensors running Windows Server 2008 R2 SP1.
  - **A group Managed Service Account (gMSA).** Requires Windows Server 2012 or above. All sensors must have permissions to retrieve the gMSA account's password.

Creating an instance

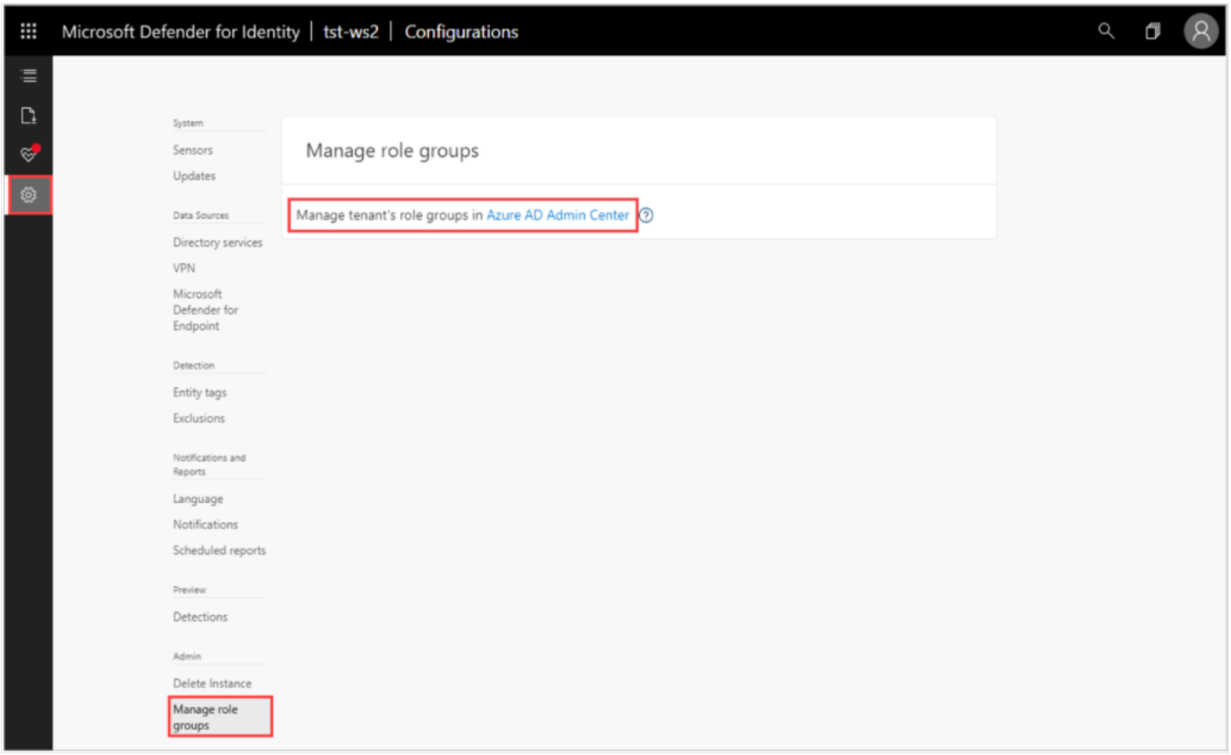
To create a Microsoft Defender for Identity instance in the Defender for identity portal, the administrator must complete the following steps:

1. Go to the Defender for Identity portal.
2. Sign in with your Microsoft 365 administrator user account.
3. On the **Welcome** page, select **Create**.


Microsoft Defender for Identity
Microsoft Defender for Identity
Create

Welcome,
You're about to create your instance of Microsoft Defender for Identity.

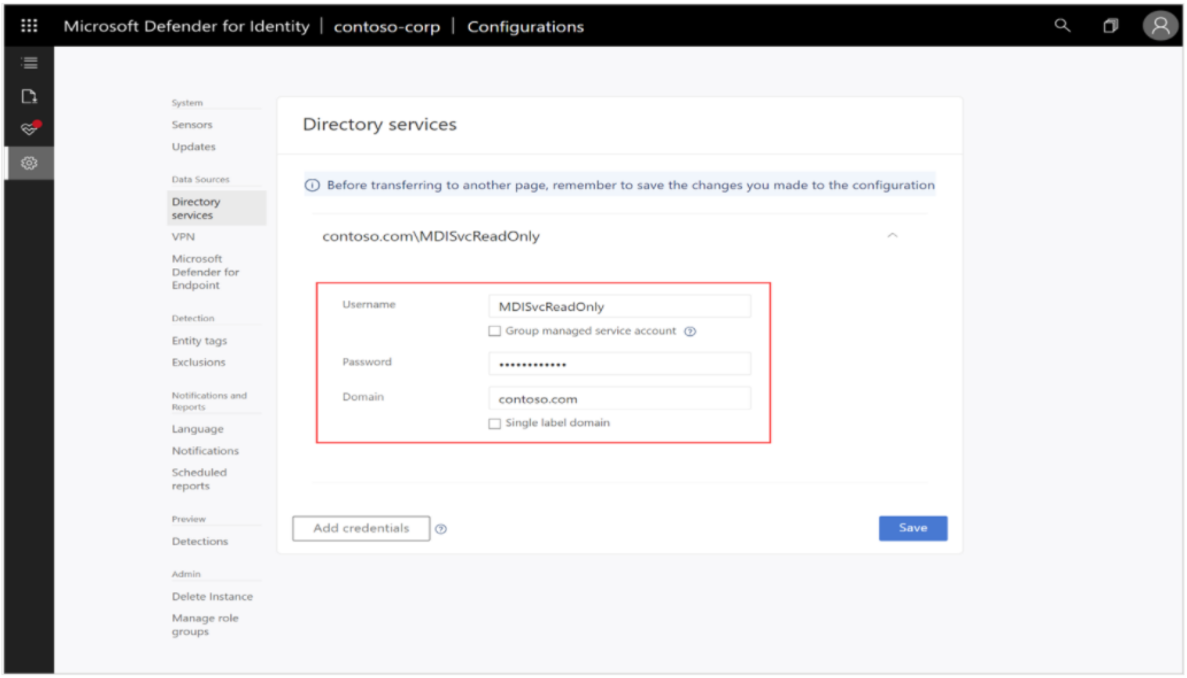
1. The Defender for Identity instance that's created is automatically named after the Azure AD initial domain name. The Defender for Identity instance is created in the data center located closest to Azure AD.
2. Select the **Configuration** (gear) icon in the left-hand navigation pane, and then select **Manage role groups**. Use the Azure AD Admin Center link to manage the role groups.



Manage role groups

Manage tenant's role groups in Azure AD Admin Center

6. Add your gMSA credentials to connect the Active Directory forest to the Microsoft Defender for identity portal.



Directory services

ⓘ Before transferring to another page, remember to save the changes you made to the configuration

contoso.com\MDISvcReadOnly

Username: MDISvcReadOnly

□ Group managed service account

Password: •••••••••••••

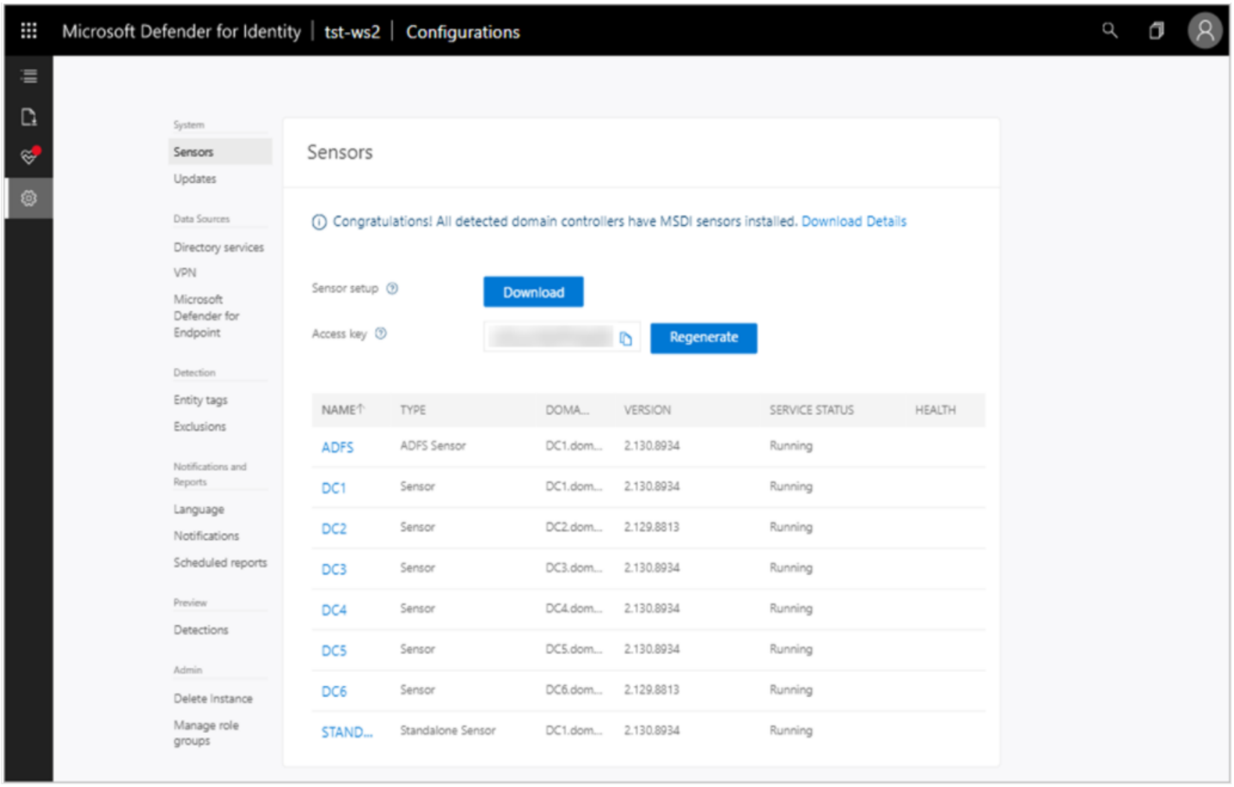
Domain: contoso.com

□ Single label domain

ⓘ **Note**

It's recommended to create a new gMSA account and security group containing all domain controllers with sensors with permissions to retrieve the gMSA account's password.

7. In the left-hand column, select **Sensors**, and then select the **Download** button and save the package locally.



Sensors

ⓘ Congratulations! All detected domain controllers have MSDI sensors installed. Download Details

Sensor setup

Access key [redacted]

NAME↑	TYPE	DOMA...	VERSION	SERVICE STATUS	HEALTH
ADFS	ADFS Sensor	DC1.dom...	2.130.8934	Running	
DC1	Sensor	DC1.dom...	2.130.8934	Running	
DC2	Sensor	DC2.dom...	2.129.8813	Running	
DC3	Sensor	DC3.dom...	2.130.8934	Running	
DC4	Sensor	DC4.dom...	2.130.8934	Running	
DC5	Sensor	DC5.dom...	2.130.8934	Running	
DC6	Sensor	DC6.dom...	2.129.8813	Running	
STAND...	Standalone Sensor	DC1.dom...	2.130.8934	Running	

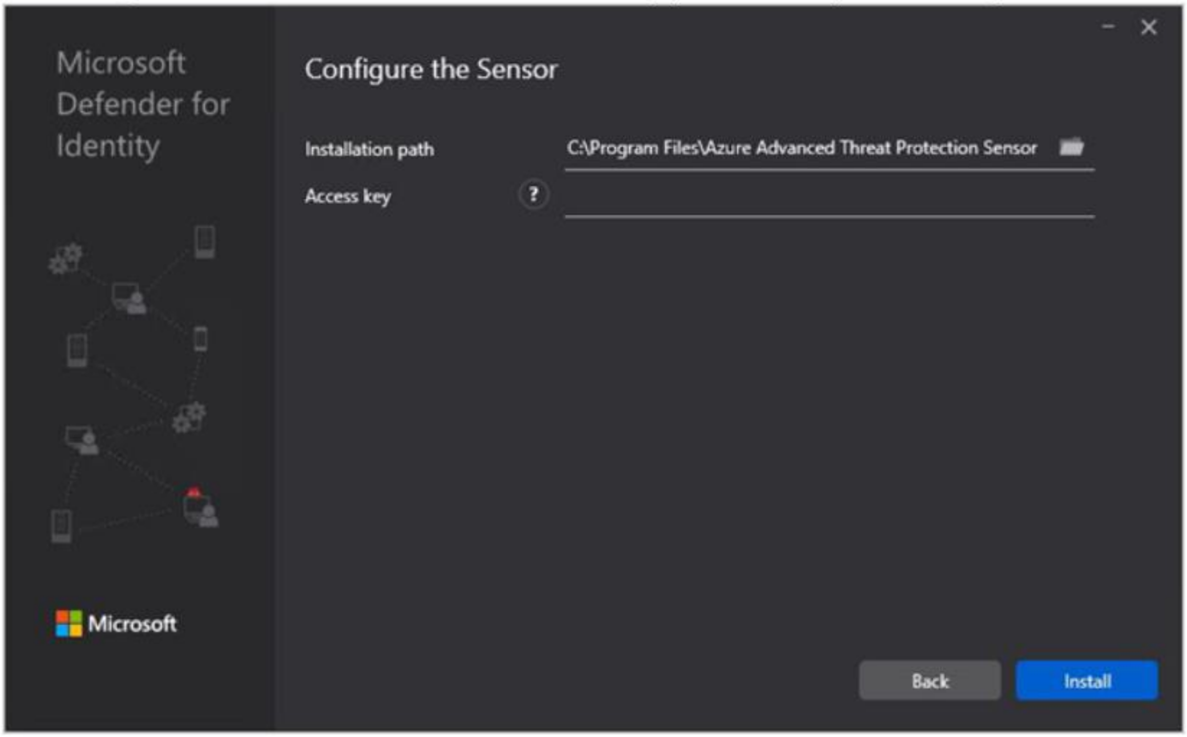
8. On the **Sensors** page (see prior screenshot image), select the **copy file** icon that appears to the right of the **Access key** field. The access key is required for the Defender for Identity sensor to connect to your Defender for Identity instance. The access key is a one-time-password for sensor deployment, after which all communication is performed using certificates for authentication and TLS encryption.

Note

Select the **Regenerate** button if you ever need to regenerate a new access key. Regenerating a new key won't affect any previously deployed sensors, because it's only used for initial registration of the sensor.

9. Copy the package to the dedicated server or domain controller onto which you're installing the Defender for Identity sensor. Alternatively, you can open the Defender for Identity portal from the dedicated server or domain controller and skip this step.
10. Verify the machine has connectivity to the relevant Defender for Identity cloud service endpoint(s).
11. Extract the installation files from the zip file. Installing directly from the zip file will fail.

12. Run **Azure ATP sensor setup.exe** with elevated privileges (**Run as administrator**) and follow the setup wizard.
13. On the **Welcome** page, select your language and select **Next**.
14. The installation wizard automatically checks if the server is a domain controller or a dedicated server to determine which sensor to install:
    - If it's a domain controller, the Defender for Identity sensor is installed.
    - If it's a dedicated server, the Defender for Identity standalone sensor is installed.
    - Select **Next.**
15. Under **Configure the sensor**, enter the installation path and the access key that you copied from the previous step, based on your environment:
    - **Installation path.** The location where the Defender for Identity sensor is installed. By default, the path is %programfiles%\Azure Advanced Threat Protection sensor. Leave the default value.
    - **Access key.** Retrieved from the Defender for Identity portal in the previous step.



Configure the Sensor

Installation path C:\Program Files\Azure Advanced Threat Protection Sensor

Access key

16. Select Install

Check your knowledge

1.

As the Enterprise Administrator for Northwind Traders, Allan Deyoung is creating an instance for Microsoft Defender for Identity. During this process, what does Allan need to have to connect the Defender for Identity sensor to Northwind's Defender for Identity instance?

○

A Microsoft Defender for Identity license

○

The access key

That's correct. The access key is required for the Defender for Identity sensor to connect to your Defender for Identity instance. The access key is a one-time-password for sensor deployment, after which all communication is performed using certificates for authentication and TLS encryption.

○

A group Managed Service Account

Microsoft Defender for Identity portal